

29. A method of claim 28, wherein step (b), further comprising steps of:

- a) Generating Variable Definition
- b) Generating statements to retrieve all dependencies
- c) Generating statements to process vulnerabilities and exposures
- d) Generating statements for passing a select set of decoded information elements
- e) Generating statements for loading a select set of decoded information elements
- f) Generating statements for flushing a select set of decoded information elements
- g) Extracting regular expressions matches, pattern matches, value list comparisons and convert them in an intermediate form that optimizes their processing

ABSTRACT OF THE DISCLOSURE

An apparatus and method for the detection and prevention of intrusions, DOS attacks, and computer worms comprising of: 1) dynamically loading information about vulnerabilities and exposures 2) intercepting application data 3) using information about vulnerabilities and exposures to detect their exploitation 4) taking custom action to stop the exploitation. Invention also includes an apparatus and method for reducing time it takes to capture information about vulnerabilities and exposures for the purpose of detecting their exploitation and stopping it. Invention further includes an apparatus and method to convert information about vulnerabilities and exposures into an intermediate form that optimizes the processing speed of the method and apparatus for stopping intrusions, DOS attacks, and computer worms.